TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/15/2016

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting the most severe of these vulnerabilities could allow for remote attackers to execute arbitrary code in the context of the affected application. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. There is known proof-of-concept code for these vulnerabilities.

SYSTEMS AFFECTED:
- PHP 7 prior to 7.0.14
- PHP 5 prior to 5.6.29

RISK:
Government:
- Large and medium government entities: **High**
- Small government: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
PHP has released updates that address multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. These vulnerabilities include:

Prior to 7.0.14
- Bug #72736 (Slow performance when fetching large dataset with mysqli / PDO).

- Bug #72978 (Use After Free Vulnerability in unserialize()). (CVE-2016-9936)
- Bug #69587 (DateInterval properties and isset).
- Bug #73526 (php_json_encode depth issue).
- Bug #64526 (Add missing mysqlnd.* parameters to php.ini-*).
- Bug #73448 (odbc_errormsg returns trash, always 513 bytes).
- Bug #69090 (check cached files permissions).
- Bug #73546 (Logging for opcache has an empty file name).
- Bug #73483 (Segmentation fault on pcre_replace_callback).
- Bug #73392 (A use-after-free in zend allocator management).
- Bug #73087, #61183, #71494 (Memory corruption in bindParam).
- Bug #73580 (Phar::isValidPharFilename illegal memory access).
- Bug #73498 (Incorrect SQL generated for pg_copy_to()).
- Bug #73538 (SoapClient::__setSoapHeaders doesn't overwrite SOAP headers).
- Bug #73452 (Segfault (Regression for #69152)).
- Bug #73423 (Reproducible crash with GDB backtrace).
- Bug #73530 (Unsetting result set may reset other result set).
- Bug #73297 (HTTP stream wrapper should ignore HTTP 100 Continue).
- Bug #73645 (version_compare illegal write access).
- Bug #73631 (Invalid read when wddx decodes empty boolean element). (CVE-2016-9935)
- Bug #72135 (malformed XML causes fault).

Prior to 5.6.29
- Bug #64526 (Add missing mysqlnd.* parameters to php.ini-*).
- Bug #73402 (Opcache segfault when using class constant to call a method).
- Bug #69090 (check cached files permissions)
- Bug #72776 (Invalid parameter in memcpy function trough openssl_pbkdf2).
- Bug #73498 (Incorrect SQL generated for pg_copy_to()).
- Bug #73452 (Segfault (Regression for #69152)).
- Bug #73530 (Unsetting result set may reset other result set).
- Bug #73297 (HTTP stream wrapper should ignore HTTP 100 Continue).
- Bug #73631 (Invalid read when wddx decodes empty boolean element). (CVE-2016-9935)

Successfully exploiting the most severe of these vulnerabilities could allow for remote attackers to execute arbitrary code in the context of the affected application. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:
- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.

REFERENCES:
NOTE: Visiting these links may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the pages below.

PHP:
http://php.net/ChangeLog-7.php
http://www.php.net/ChangeLog-5.php

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9936
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9935